Gli assiomi di $\mathbb{R}$ e alcune proprietà elementari

L'insieme dei numeri reali $\mathbb{R}$ è un insieme non vuoto dotato di due operazioni binarie[1], somma (denotata con "$+$") e prodotto (denotata con "$\cdot$") e di una relazione[2] d'ordine $\mathcal{R}$ (denotata "$\leq$") tale che valgono i seguenti assiomi:

Assiomi della addizione:
(S$_1$) $x + y = y + x \quad \forall\, x, y \in \mathbb{R}$ — proprietà commutativa di $+$;
(S$_2$) $(x + y) + z = x + (y + z) \quad \forall\, x, y, z \in \mathbb{R}$ — proprietà associativa di $+$;
(S$_3$) $\exists\, 0 \in \mathbb{R}$ tale che $x + 0 = x \quad \forall\, x \in \mathbb{R}$ — esiste elemento neutro per $+$;
(S$_4$) $\forall\, x \in \mathbb{R},\ \exists\, y \in \mathbb{R}$, tale che $x + y = 0$ — esistenza elemento opposto.

Assiomi della moltiplicazione:
(P$_1$) $x \cdot y = y \cdot x \quad \forall\, x, y \in \mathbb{R}$ — proprietà commutativa di $\cdot$;
(P$_2$) $(x \cdot y) \cdot z = x \cdot (y \cdot z) \quad \forall\, x, y, z \in \mathbb{R}$ — proprietà associativa di $\cdot$;
(P$_3$) $\exists\, 1 \in \mathbb{R}, 1 \neq 0$, tale che $x \cdot 1 = x \quad \forall\, x \in \mathbb{R}$ — esiste elemento neutro per $\cdot$;
(P$_4$) $\forall\, x \in \mathbb{R},\ x \neq 0,\ \exists\, y \in \mathbb{R}$ tale che $x \cdot y = 1$ — esistenza del reciproco.

Proprietà distributiva:
(SP) $x \cdot (y + z) = (x \cdot y) + (x \cdot z) \quad \forall\, x, y, z \in \mathbb{R}$.

Assiomi di ordine[3] totale:
(O$_1$) $x \leq x \quad \forall\, x \in \mathbb{R}$ — proprietà riflessiva di $\leq$;
(O$_2$) $x \leq y,\ y \leq x$ allora $x = y$ — proprietà antisimmetrica di $\leq$;
(O$_3$) $x \leq y,\ y \leq z$ allora $x \leq z$ — proprietà transitiva di $\leq$;
(O$_4$) $x \leq y$ o $y \leq x \quad \forall\, x, y \in \mathbb{R}$ — ordine totale di $\leq$.

Assioma di somma e ordine:
(SO) $x \leq y$ allora $x + z \leq y + z \quad \forall\, z \in \mathbb{R}$.

Assioma di prodotto e ordine:
(PO) $0 \leq x,\ 0 \leq y$ allora $0 \leq x \cdot y$.

Proposizione 1 (i) (Unicità dell'opposto) *Se* $x + y = 0$ *e* $x + z = 0$ *allora* $y = z$.
(ii) (Unicità del reciproco) *Se* $x \cdot y = 1$ *e* $x \cdot z = 1$ *allora* $y = z$.

Dimostrazione (i): $y \overset{(S_3)}{=} y + 0 = y + (x + z) \overset{(S_2)}{=} (y + x) + z \overset{(S_1)}{=} (x + y) + z = 0 + z = z$.
(ii) $y = y \cdot 1 = y \cdot (x \cdot z) = (y \cdot x) \cdot z = (x \cdot y) \cdot z = 1 \cdot z = z$. ∎

Notazioni: L'opposto di x si denota con $-x$; $y + (-x)$ si denota $y - x$. Il reciproco di $x \neq 0$ si denota con x^{-1} o con $1/x$ o con $\dfrac{1}{x}$; $x \cdot y^{-1}$ si denota anche con x/y o con $\dfrac{x}{y}$. $2 := 1 + 1$; $x^2 := x \cdot x$. $x \geq y$ è equivalente a $y \leq x$; $x < y$ significa $x \leq y$ e $x \neq y$; $x > y$ è equivalente a $y < x$. $x + y \cdot z := x + (y \cdot z)$.

[1] Una operazione binaria su $\mathbb{R}$ è una funzione da $\mathbb{R} \times \mathbb{R}$ in $\mathbb{R}$.
[2] Una "relazione" in un insieme A è un sottoinsime di $A \times A$; nel caso della relazione d'ordine $\mathcal{R}$ di $\mathbb{R}$ è uso comune scrivere al posto di $(x, y) \in \mathcal{R}$, $x \leq y$.
[3] Una relazione che soddisfi esclusivamente le proprietà riflessiva, antisimmetrica e transitiva, si dice relazione di "ordine parziale". Un ordine parziale è totale quando tutti gli elementi sono in relazione.

Proposizione 2 (i) (Legge di cancellazione per la somma) *Se $x + y = x$ allora $y = 0$.*

(ii) (Legge di cancellazione per il prodotto) *Se $x \neq 0$ e $x \cdot y = x$ allora $y = 1$.*

(iii) *$x \cdot 0 = 0$ per ogni x.*

(iv) *$(-1) \cdot x = -x$.*

(v) *Se $x \geq 0$ allora $-x \leq 0$; se $x \leq 0$ allora $-x \geq 0$.*

(vi) *$-(-x) = x$.*

(vii) *$x^2 \geq 0$ per ogni x.*

(viii) *$1 > 0$.*

Dimostrazione (i): $y = y + 0 = y + (x - x) = (y + x) - x = (x + y) - x = x - x = 0$.
(ii): $y = y \cdot 1 = y \cdot (x \cdot x^{-1}) = (y \cdot x) \cdot x^{-1} = (x \cdot y) \cdot x^{-1} = x \cdot x^{-1} = 1$.
(iii): $x \cdot 0 = x \cdot (0 + 0) = x \cdot 0 + x \cdot 0$ che implica per (i) $x \cdot 0 = 0$.
(iv): $x + (-1) \cdot x = 1 \cdot x + (-1) \cdot x = (1 - 1) \cdot x = 0 \cdot x = 0$ e dall'unicità dell'opposto segue che $-x = (-1) \cdot x$.
(v): $x \geq 0$ implica (per (SO)) $x - x \geq -x$ ossia $0 \geq -x$; $x \leq 0$ implica (per (SO)) $x - x \leq -x$ ossia $0 \leq -x$.
(vi): $(-x) + x = x - x = 0$ quindi dall'unicità dell'opposto segue che $-(-x) = x$.
(vii): Se $x \geq 0$ l'asserto deriva da (PO). Sia ora $x \leq 0$, allora $x^2 = x \cdot x = (-(-x)) \cdot x = (-1 \cdot (-x)) \cdot x = (-x) \cdot ((-1) \cdot x) = (-x) \cdot (-x) \geq 0$ per (PO) essendo per (v) $-x \geq 0$.
(viii): $1 = 1 \cdot 1 \geq 0$ e per (P_3) $1 \neq 0$ quindi $1 > 0$. ∎

Assioma dell'esistenza dell'estremo superiore

Definizione 3 (i) *Un maggiorante M di un insieme $A \subseteq \mathbb{R}$ non vuoto, è un numero reale tale che $M \geq x$, per ogni $x \in A$.*

(ii) *Sia $A \subseteq \mathbb{R}$ non vuoto. Se esiste $M \in A$ tale che $x \leq M$ per ogni $x \in A$, tale numero $M =: \max A$ si chiama il massimo di A.*

(iii) *Un insieme $A \subseteq \mathbb{R}$ si dice limitato superiormente se esiste un maggiorante di A.*

(iv) *Dato un insieme non vuoto $A \subseteq \mathbb{R}$ limitato superiormente, diremo che $s =: \sup A$ è l'estremo superiore di A (o che A ammette estremo superiore s) se s è un maggiorante di A e se $s \leq M$ per ogni maggiorante M di A.*

(ES) Assioma dell'estremo superiore
Ogni insieme $A \subseteq \mathbb{R}$ non vuoto e limitato superiormente ammette estremo superiore.

Osservazione 4 (i) L'estremo superiore di un insieme non vuoto, limitato superiormente è unico (esercizio).

(ii) Se un insieme ammette massimo, tale massimo coincide con l'estremo superiore. Chiaramente, il massimo di un insieme A non vuoto, limitato superiormente può non esistere ed in tal caso $\sup A \notin A$.

(iii) Definizioni analoghe (simmetriche) si danno per *minoranti*, *minimo* e per l'*estremo inferiore*[4]. Si noti (esercizio) che $\inf A = -\sup(-A)$ dove l'insieme $-A$ è definito come $-A := \{y = -x : x \in A\}$. Quindi l'estremo inferiore esiste sempre grazie a **(ES)**.

[4] Un minorante di un insieme $A \subseteq \mathbb{R}$ è un numero m tale che $m \leq x$ per ogni $x \in A$; il minimo di A (qualora esista) è un numero $m \in A$ tale che $m \leq x$ per ogni $x \in A$; un insieme si dice *limitato inferiormente* se ha un minorante; l'estremo inferiore $r = \inf A$ di un insieme A non vuoto e limitato inferiormente è un minorante r tale che $r \geq m$ per ogni minorante m di A.

Si ha la seguente caratterizzazione dell'estremo superiore.

Proposizione 5 $s = \sup A$ *se e solo se* s *è un maggiorante per* A *e per ogni* $t < s$ *esiste un elemento* x *di* A *tale che* $t < x$*.*

Dimostrazione Se $s = \sup A$, s è un maggiorante di A e quindi $x \leq s$ per ogni $x \in A$. Sia $t < s$. Se $x \leq t$ per ogni $x \in A$, si avrebbe che t è un maggiorante di A strettamente più piccolo di s contraddicendo la definizione di estremo superiore. Quindi esiste $x \in A$ con $x > t$. Sia ora s un maggiorante per A tale che per ogni $t < s$ esiste un elemento x di A con $t < x$. Chiaramente non può esistere un maggiorante $M < s$ (si prenda $t = M$) e quindi $s = \sup A$. ∎